أفضل تطبيق آمن للمراسلة

كيف تختار تطبيق المراسلة الذي تستخدمه؟

إعداد: مجلس التعاون الإعلامي الإسلامي

تقديم: جيش الملاحم الإلكتروني



Al-Malahem Electronic Army

بسم الله الرحمن الرحيم

جيش الملاحم الإلكتروني

يقدم

ما هو أفضل تطبيق آمن للمراسلة

كيف تختار تطبيق المراسلة الذي تستخدمه

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

المصدر

/https://nordvpn.com/blog/most-secure-messaging-app

فهرس المحتويات

المقدمة

يحافظ تطبيق المراسلة الآمن، مثل WhatsApp، على خصوصية محادثاتك. ولكن كم ماهي دقة هذا الوصف؟! سواء كانت قصة محرجة، أو ثرثرة في المكتب، أو الانفتاح على مشاعرك، فإن آخر شيء تريده هو أن يرى شخص ما رسائلك أو يستخدمها لعرض إعلاناتك. ما لم تكن تستخدم تطبيق مراسلة مشفر، فإنك تترك كل شيء في العلن.

بينما يلعب التشفير والخصوصية دورًا حيويًا في اختيار تطبيق المراسلة الذي سيتم استخدامه، فمن الضروري أيضًا استخدام تطبيقات المراسلة التي يستخدمها أصدقاؤنا.

وفقًا لـ Statista (2022)، تظل WeChat وWhatsApp وFacebook Messenger أكثر تطبيقات المراسلة شيوعًا في العالم على الرغم من ممارسات الخصوصية المشكوك فيها لدى Facebook.

تطبيقات المراسلة الأكثر شعبية حسب البلد

Germany	WhatsApp **95%**
China	WeChat **81%**
Spain	WhatsApp **92%**
Italy	WhatsApp **97%**
France	FB Messenger **59%**
Denmark	FB Messenger **72%**
Finland	WhatsApp **95%**
Sweden	FB Messenger **64%**
UK	WhatsApp **71%**
US	FB Messenger **83%**
India	WhatsApp **97%**
Singapore	WhatsApp **83%**
Austria	WhatsApp **94%**
Brazil	WhatsApp **99%**

- يستخدم تطبيق WhatsApp ما يزيد عن 90% من الأشخاص في البلدان التي يعتبر فيها تطبيق المراسلة الرائد. في الواقع، يعد تطبيق WhatsApp هو تطبيق المراسلة الأكثر استخدامًا على مستوى العالم.

- في عام 2022، يستخدم حوالي 83% من الولايات المتحدة تطبيق Facebook Messenger، في حين يختار غالبية سكان أمريكا اللاتينية تطبيق WhatsApp.

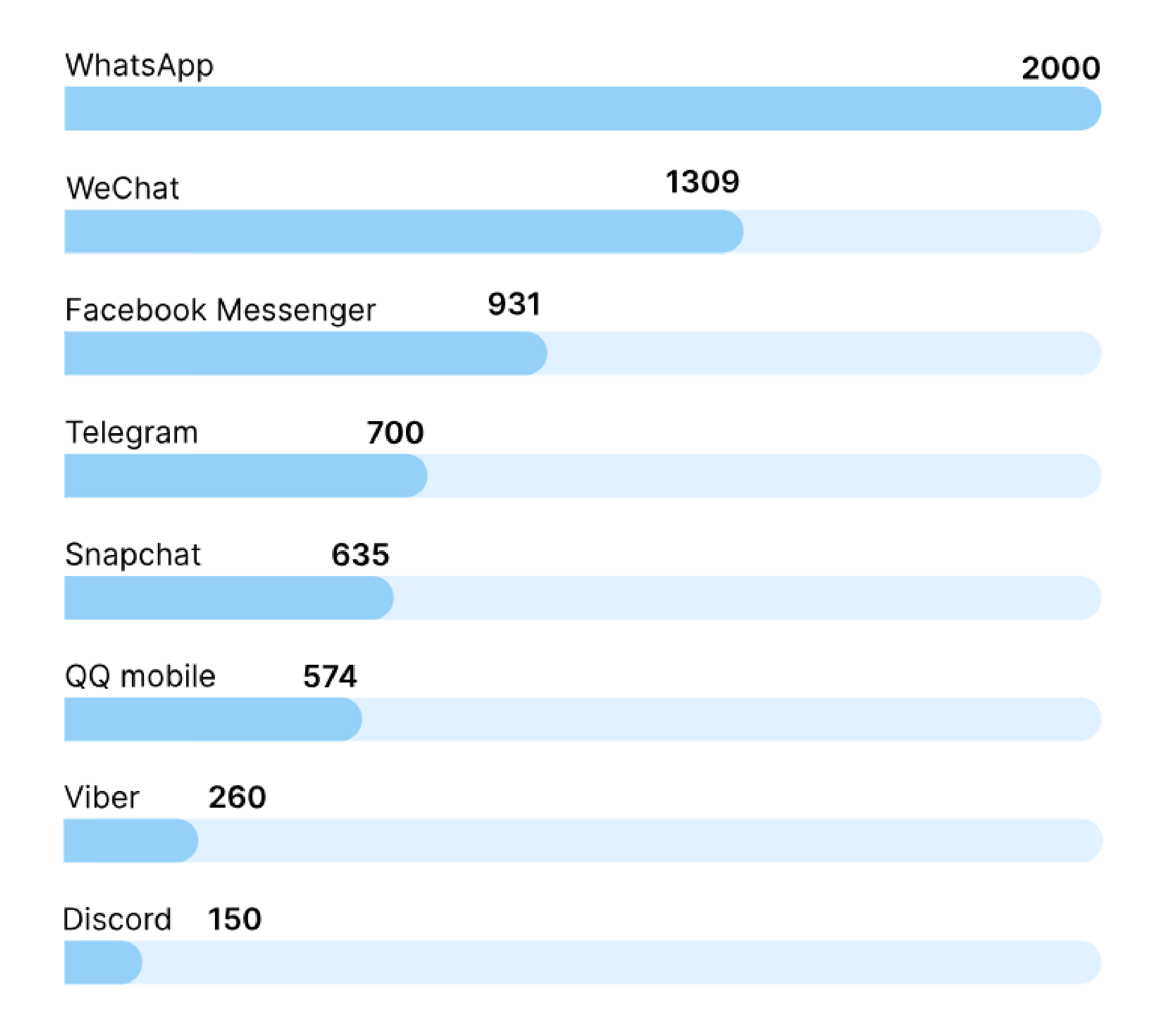
- يمتلك فيسبوك اثنتين من الشركات الرائدة في السوق (WhatsApp و Facebook Messenger)، مما يعني أن معظم العالم يستخدم تطبيقات المراسلة المملوكة لفيسبوك.

- يستخدم WeChat غالبية الأشخاص في الصين، نظرًا لأن تطبيقات مثل WhatsApp وFacebook Messenger محظورة.

- يواجه تطبيق Telegram، المعروف بضوابطه الصارمة على الخصوصية، صعوبة في الحصول على جاذبية جماهيرية، حيث أن معظم مستخدميه يقيمون في الشرق الأوسط.

- أصبح الأمان والخصوصية داخل تطبيقات المراسلة أكثر أهمية. إذا كان الأمان هو نقطة اهتمامك الأولى بدلاً من الشعبية، فتابع القراءة.

أكثر تطبيقات المراسلة شعبية بناءً على عدد المستخدمين النشطين شهريًا (بالملايين)



WhatsApp 2000 , WeChat 1309 , Facebook Messenger 931 , Telegram 700 , Snapchat 635 , QQ mobile 574 , Viber 260 , Discord 150

كيفية اختيار تطبيق المراسلة الآمن

اختر تطبيقًا يستخدم التشفير الشامل والتعليمات البرمجية مفتوحة المصدر ولا يخزن بياناتك.

العديد من تطبيقات المراسلة المتوفرة في السوق ليست كلها آمنة كما يدعون في الواقع، حتى تطبيق المراسلة الأكثر شيوعًا في العالم ليس محصنًا ضد عمليات الاحتيال (راجع عمليات الاحتيال على WhatsApp).

لتسهيل اختيارك، قمنا بتجميع قائمة من التطبيقات التي توفر التشفير الشامل، مما يعني أنه لا يمكن لأحد رؤية محادثاتك ما لم يكن لديه مفتاح خاص لفك تشفير رسالتك.

والأهم من ذلك، أن هذا يعني أنه حتى مقدم الخدمة لا يمكنه رؤية رسائلك - ولا حتى أصحاب العمل المسيئين، أو المتسللين، أو المسؤولين الحكوميين. ومع ذلك، فإن ميزاتها الإضافية وعيوبها كلها مختلفة.

لقد قمنا بمراجعة 10 تطبيقات مراسلة مشفرة وعرضنا إيجابياتها وسلبياتها.

Viber

الإيجابيات	السلبيات
تشفير E2E تشفير كامل بمفاتيح تشفير لا يمكن فكها إلا من قبل المتلقي	يجمع البيانات حول المستخدمين وجهات الاتصال الخاصة بهم **(عيب خطير، ليس الأفضل للخصوصية)**
رسائل التدمير الذاتي	يتتبع نشاط المستخدمين على وسائل التواصل الاجتماعي **(عيب أمني خطير لتتبع المستخدمين)**
دعم واسع للجهاز	

تم تصميم Viber، وهو أحد أقوى منافسي WhatsApp، في البداية لإجراء مكالمات عبر الإنترنت ولكنه سرعان ما تطور ليصبح تطبيق دردشة متكامل.

يمكنك استخدامه لإرسال الرسائل الصوتية والنصية والصور ومقاطع الفيديو إلى مستخدمين ومجموعات من المستخدمين الآخرين. جميع الدردشات، بما في ذلك الدردشات الجماعية، مشفرة بالكامل.

مكنك استخدام Viber على الأجهزة المحمولة ومعظم أنظمة تشغيل سطح المكتب.

ومع ذلك، فإن إحدى ميزات Viber الأكثر جاذبية هي رسائل التدمير الذاتي. ولكن هذا هو المكان الذي تنتهي فيه الأخبار الجيدة..

تشتهر الشركة بجمع الأسماء وأرقام هواتف مستخدميها الفرديين بالإضافة إلى الأشخاص الموجودين في قوائم الاتصال الخاصة بالمستخدمين، حتى لو كان هؤلاء الأشخاص لا يستخدمون فايبر. يذهب Viber إلى حد متابعة نشاط مستخدميه على الشبكات الاجتماعية. فهو يستخدم جميع البيانات الوصفية التي يمكنه الحصول عليها، لذا فإن استخدام خدمات فايبر يعد أمرًا محفوفًا بالمخاطر.

WhatsApp

الإيجابيات	السلبيات
يستخدم تشفير Signal	مملوكة للفيسبوك **(الشركة مشهورة بجمع البيانات ونشاطات المستخدمين وتتبعهم وانتهاك خصوصيتهم)**
من المحتمل أن معظم أصدقائك يستخدمونه	شهدت خرقا كبيرا **(حوادث اختراق سابقة وثغرات أمنية)**
سهل الاستخدام ويوفر ميزات إضافية	

مع أكثر من مليار مستخدم، يعد تطبيق WhatsApp أحد تطبيقات المراسلة الأكثر استخدامًا على نطاق واسع. إنه سهل الاستخدام ويوفر ميزات مثل مشاركة الموقع والملفات والصور المتحركة وحتى دعم سطح المكتب. كما أنه يستخدم بروتوكول التشفير القوي الذي تم تطويره لـ Signal بواسطة Open Whisper Systems، والذي يعتبر معيار الصناعة.

يتميز التشفير بالسرية التامة للأمام (PFS). وهذا يعني أنه إذا تمكن شخص ما من سرقة مفتاح فك التشفير لمحادثتك، فلن يتمكن إلا من رؤية الرسالة الأخيرة التي أرسلتها. كل شيء آخر سيبقى خاصا..

ومن ناحية أخرى، فإن تطبيق WhatsApp مملوك لشركة Facebook، مما يثير مخاوف أمنية كبيرة. يقع جمع بيانات المستخدمين في قلب نموذج أعمال عملاق التواصل الاجتماعي، وقد فشل في الحفاظ على أمان بيانات المستخدم عدة مرات. هل يمكننا حقًا أن نثق بفيسبوك، على الرغم من التشفير الآمن؟

في 14 مايو 2019، اكتشف المتسللون ثغرة أمنية خطيرة في تطبيق WhatsApp واستخدموها لتثبيت برامج ضارة للمراقبة على عدد محدد من الهواتف. تم إدخال برنامج التجسس هذا من خلال مكالمات WhatsApp الصوتية (لم يكن الشخص المستهدف بحاجة إلى الرد على المكالمة) ومنح المتسللين إمكانية الوصول إلى الرسائل النصية للضحايا، ورسائل البريد الإلكتروني، ورسائل WhatsApp، وتفاصيل الاتصال، وسجلات المكالمات، والموقع، والميكروفون، والكاميرا. لقد تم الآن تصحيح الثغرة الأمنية.

(الدراسة هنا تقصد برنامج بيجاسوس الإسرائيلي)

Facebook Messenger

الإيجابيات	السلبيات
ربما يستخدمه معظم أصدقائك	التشفير ليس افتراضيًا **(يجب عليك تفعيل خيار التشفير يدوياً والذي قد يكون بحد ذاته عملية فرز بيانات لمعرفة من مهتم بالتشفير عن البقية)**
يمكنك استخدامه حتى لو قمت بإلغاء تنشيط حسابك على Facebook	لا يقوم بتشفير المحادثات السابقة
	يتتبع سلوكك **(خطر كبير في انتهاك الخصوصية)**

يستخدم مليارات الأشخاص فيسبوك وخدمات المراسلة الخاصة به، لكن القليل منهم يعلم أن تطبيق الشركة يوفر ميزة التشفير التام بين الطرفين. وذلك لأن Facebook قام بعمل رائع في إخفاء هذه الميزة. (تعرف على كيفية بدء محادثة سرية على Facebook هنا)
https://nordvpn.com/blog/facebook-secret-conversation/

من المثير للإعجاب أن فيسبوك قدم هذه الميزة، لكن هذا لا يغير حقيقة أن عملاق الوسائط الاجتماعية يجمع بيانات مثل من تراسله أو عدد مرات استخدامك للتطبيق. ودعونا لا ننسى أنه في عام 2018، أصبح فيسبوك مشهورًا بسبب خروقاته المتعددة للبيانات. أصبح من الصعب الوثوق بخصوصية محادثاتك.!

iMessage

الإيجابيات	السلبيات
يتشغل التشفير بشكل افتراضي	جمع معلومات المستخدم بناءً على سلوكهم **(عيب خطير في انتهاك الخصوصية)**
برنامج سطح مكتب سهل الاستخدام	فشل في تشفير البيانات الحساسة الأخرى مثل أرقام الهواتف المحمولة أو البيانات الوصفية أو البيانات المخزنة في السحاب
دعم واسع للجهاز	

ليس هناك شك في أن منتجات Apple تتمتع بسمعة جيدة عندما يتعلق الأمر بالأمن السيبراني. البديل الذي يستخدمه أصحاب iPhone للرسائل النصية – iMessage – لديه تشفير افتراضي بين الطرفين. ومع ذلك، فإنه لا يزال يحتوي على العديد من نقاط الضعف وهو بعيد عن منصة المراسلة الأكثر أمانًا.

يتم تخزين المعلومات مثل أرقام الهواتف المحمولة وقوائم جهات الاتصال بنص عادي بدلاً من التجزئة، كما هو الحال مع الطوابع الزمنية وعناوين IP. يفشل التطبيق أيضًا في تشفير بياناتك التعريفية وأي بيانات تمت مزامنتها مع iCloud. إذا قام أي شخص باختراق السحابة الخاصة بك، فسيكون لديه إمكانية الوصول الخلفي إلى جهازك..

Telegram

الإيجابيات	السلبيات
يقدم رسائل تختفي وميزات إضافية أخرى	على الرغم من أن التطبيق مفتوح المصدر، إلا أن خوادمه ليست كذلك **(الكود مفتوح المصدر ولكن لا أحد يعلم ما يحدث داخل الخوادم إلا الشركة فقط)**
واجهة سهلة الاستخدام	التشفير ليس افتراضيًا **(عليك تفعيل الإعدادات يدوياً أو عمل محادثة مشفرة)**
	يستخدم بروتوكول التشفير الخاص

أكثر من 100 مليون شخص يستخدمون Telegram. صحيح أن المنصة سهلة الاستخدام، وتوفر العديد من الميزات الإضافية، وليست ملزمة بإعطاء أي معلومات عن المستخدم لوكالات الاستخبارات (على حد علمنا). ومع ذلك، فإن Telegram ليس آمنًا كما يريدنا أن نصدق.

أولاً، يبدو من الغريب أن تطبيق المراسلة الموجه نحو الأمان هذا لا يحتوي على تشفير افتراضيًا. العديد من الأشخاص الذين يستخدمون Telegram لا يدركون هذه المشكلة، مما يتعارض مع الغرض من التطبيق.

بروتوكول تشفير Telegram معيب أيضًا. تم تطويره من قبل فريق داخلي يتمتع بخبرة قليلة في مجال التشفير. خوادم Telegram ليست مفتوحة المصدر، لذلك لم يتم تدقيق الكود من قبل أطراف ثالثة. كما أن الشركة لا تقدم تقارير الشفافية.

(في اشارة الدراسة إلى أن تطبيق تلجرام لا يشارك المعلومات مع وكالات الاستخبارات والقول على حد علمنا بين قوسين، اشارة مباشرة إلى شكوك تدور حول التطبيق وتعاملاته مع جهات استخباراتية، ولكن بالطبع الدراسة لا يمكنها التصريح بهذا بشكل مباشرة إنما تلمح إليه)

تابع القراءة للاطلاع على أفضل ثلاثة تطبيقات للمراسلة الآمنة، أو شاهد هذا الفيديو الذي يشرح سبب اختيارنا لها.

https://www.youtube.com/watch?v=frgkHVJKVq4

Silence

الإيجابيات	السلبيات
حل آمن للرسائل النصية القصيرة/رسائل الوسائط المتعددة	لأجهزة الأندرويد فقط
مجانا للجميع	لا يوجد دعم مباشر
لا لقطة للشاشة	قاعدة مستخدمين محدودة
لا يلزم الاتصال بالإنترنت	

تطبيق Silence هو تطبيق SMS/MMS آمن يمكنك استخدامه حتى إذا لم تكن متصلاً بالإنترنت.

يمكنك إرسال رسائل إلى أي شخص، وليس فقط مستخدمين Silence .

ومع ذلك، لا يتوفر التشفير الشامل إلا عند إرسال رسائل نصية إلى مستخدمي تطبيق Silence الآخرين.

وهو متوفر على أجهزة Android فقط.

يتم تشفير جميع الرسائل المخزنة على هاتفك، ولا تتذكر لوحة المفاتيح المتخفية سجل الكتابة الخاص بك، ويمنع خيار شاشة الأمان المستخدمين من التقاط لقطات الشاشة.

من الناحية الأمنية، يعد Silence واحدًا من أكثر تطبيقات المراسلة أمانًا، ولكن إذا كنت تبحث عن ميزات أكثر تطورًا مثل مكالمات الفيديو، فسيتعين عليك البحث في مكان آخر.

Threema

الإيجابيات	السلبيات
لا يخزن البيانات أو يسجل عناوين IP	قاعدة مستخدمين محدودة
يحفظ الحد الأدنى من البيانات الوصفية	لا توجد نسخة مجانية
لا يتعين عليك تقديم البريد الإلكتروني أو رقم الهاتف للتسجيل	
الرسائل وجهات الاتصال المخزنة على جهاز المستخدم بدلاً من الخوادم	

هو تطبيق مراسلة مشفر مدفوع الأجر يوفر مستوى عالٍ من إخفاء الهوية. فهو يوفر رسائل نصية وصوتية خاصة ومكالمات صوتية ومرئية واستطلاع جماعي ومشاركة الملفات. ليس عليك حتى تقديم عنوان بريدك الإلكتروني أو رقم هاتفك للتسجيل. بدلاً من ذلك، يتم تعيين معرف تم إنشاؤه عشوائيًا. يمكنك التحقق من جهات الاتصال الخاصة بك من خلال رمز الاستجابة السريعة.

يتم حذف رسائلك من خوادم Threema بمجرد تسليمها، دون ترك أي أثر. لا يتم تخزين البيانات الوصفية، باستثناء أصغر كمية مطلوبة لتشغيل التطبيق.

بشكل عام، توفر Threema خدمات آمنة للغاية وترسل برامجها لعمليات التدقيق الخارجية لتأكيدها، مما يجعلها واحدة من أكثر تطبيقات المراسلة أمانًا على الإطلاق.

هناك عيب واحد، ربما مؤقت، وهو قلة عدد المستخدمين – حوالي 11 مليونًا فقط في الربع الأخير من عام 2022.

Wire

السلبيات	الإيجابيات
يجمع بعض البيانات عن مستخدميه **(عيب خطير، ليس الأفضل للخصوصية)**	مفتوح المصدر
	يتوافق مع قوانين البيانات في الاتحاد الأوروبي
	يمكن استخدامه على غالبية متصفحات الإنترنت

للوهلة الأولى، يحقق Wire جميع متطلبات تطبيق المراسلة الآمن - فهو يوفر تشفيرًا شاملاً، ويتوافق مع جميع قوانين البيانات والخصوصية في الاتحاد الأوروبي، كما أنه مفتوح المصدر، وليس ملزمًا بمشاركة بياناته مع خدمات المراقبة. بالإضافة إلى ذلك، يمكنك استخدامه على معظم المتصفحات الشائعة مثل Firefox وChrome وSafari وOpera. ومع ذلك، يقوم Wire بجمع وتخزين بعض بيانات المستخدم.

اعترف منشئوا التطبيق بالاحتفاظ بسجلات للأشخاص الذين اتصل بهم المستخدمون، ولسوء الحظ يتم حفظها كلها بنص عادي. كما يقوم أيضًا بتخزين عناوين البريد الإلكتروني للمستخدمين وأرقام هواتفهم وأسماء المستخدمين. ووفقا لـ Wire، فإن هذه المعلومات تجعل مزامنة الجهاز أسهل ويتم حذفها بمجرد إلغاء تنشيط الحساب.

Wickr

الإيجابيات	السلبيات
لا تحتاج إلى رقم هاتف أو عنوان بريد إلكتروني للتسجيل	قد يكون من الصعب التبديل من منصات المراسلة الأخرى اليه
مفتوح المصدر	
يقدم ميزة "التقطيع"	
لا يجمع بيانات المستخدم أو يخزن البيانات الوصفية	
يقدم نسخة برو للشركات	

يعد Wickr أحد أفضل تطبيقات المراسلة الآمنة في السوق. إنه مفتوح المصدر ولا يجمع بيانات المستخدم أو البيانات الوصفية. كما يوفر أيضًا ميزة "التقطيع"، التي تقوم تلقائيًا بحذف جميع المحادثات والملفات التي تمت مشاركتها على النظام الأساسي.

يمكنك ضبط مؤقت لوقت حذفها. والأهم من ذلك، أنك لا تحتاج إلى رقم هاتف أو عنوان بريد إلكتروني للتسجيل، لذلك من الأسهل الحفاظ على خصوصية حياتك.

الجانب السلبي الوحيد هو أن Wickr لا يحظى بشعبية مثل Signal أو Telegram. تم تصميمه في البداية للشركات والمؤسسات، لذلك لم يتم الإعلان عنه على نطاق واسع للمستخدمين العاديين.

لا يزال Wickr يقدم إصدار Pro مدفوع حيث يمكنك إجراء مكالمات فيديو جماعية مشفرة، وهو شيء لا يقدمه أي تطبيق آخر حاليًا.

إذا لم تكن رائد أعمال وترغب في استخدام Wickr، فستحتاج إلى إقناع أصدقائك بالتحرك أيضًا.

Signal

الإيجابيات	السلبيات
يتعامل مع الدردشات الجماعية والرسائل النصية القصيرة والصوت والفيديو والمستندات والرسائل المصورة	يحتاج إلى رقم هاتف للتسجيل **(ليس عيب خطير حيث يمكن استخدام الرقم الوهمي)**
يقدم رسائل تختفي (مع مؤقت)	
بروتوكول الإشارة	
مفتوح المصدر	
لا يخزن بيانات المستخدم أو البيانات الوصفية	
دافع عنه إدوارد سنودن	

هو الأفضل من بين باقي التطبيقات لكل من مستخدمي iOS وAndroid.

أنشأ Signal بروتوكول تشفير يُعرف الآن بأنه بروتوكول تطبيق المراسلة الأكثر أمانًا المتاح. إنه يوفر كل ما يحتاجه معظم المستخدمين - الرسائل القصيرة ومكالمات الفيديو والصوت والمحادثات الجماعية ومشاركة الملفات واختفاء الرسائل - دون حشو التطبيق بالإعلانات وجمع بيانات المستخدم.

إنها أيضًا منصة مفتوحة المصدر بحيث يمكن لأي شخص التحقق من نقاط الضعف فيها.

بالحديث عن ذلك، ربما عثرت شركة أمنية إسرائيلية على ثغرة أمنية محتملة، ولهذا السبب من الأفضل دائمًا استخدام VPN جنبًا إلى جنب مع تطبيقات المراسلة الآمنة المفضلة لديك.

(الدراسة هنا تشير إلى تطبيق بيجاسوس الإسرائيلي)

المقارنة بين التطبيقات



Comparison						wickr				
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓	–	–	–
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓	✓	✗	–
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Open source apps	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Open source servers	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Personal information is hashed	✗	✗	✗	✗	–	✓	–	✓	–	–
Encrypts metadata	✗	✗	✗	✗	–	✓	✓	–	–	–
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	–	✓	✓	✓	–	–

رفض التعاون مع وكالات الاستخبارات، يقدم تقارير الشفافية، يمتنع عن جمع بيانات المستخدم، التشفير الافتراضي، تطبيقات مفتوحة المصدر، خوادم مفتوحة المصدر، تتم تجزئة المعلومات الشخصية، البيانات الوصفية المشفرة، لا يسجل الطوابع الزمنية وعناوين IP

في الصورة أعلاه لاحظ أن تطبيقات مثل ماسنجر فيس بوك وواتس أب مثلا مشهورة جداً بتعمالها مع أجهزة الإستخبارات وتقديم البيانات لهم عند طلبها.

لاحظ كذلك أن تطبيق مثل سينجنال قد اجتاز جميع الإختبارات الأمنية بنجاح وحقق جميع المتطبيات.

هل تحتاج إلى تطبيق مراسلة مشفر؟

نعم، أنت بحاجة إلى استخدام أحد أفضل تطبيقات المراسلة المشفرة لأن التشفير يحمي اتصالاتك من الاعتراض. يمكن للأطراف الثالثة قراءة الرسائل غير المشفرة بسهولة، بينما تتمتع الرسائل المشفرة بطبقة إضافية من الحماية.

التشفير من طرف إلى طرف (E2E) يعني أن مستلمي الرسالة فقط هم من يمكنهم قراءتها لأنهم الوحيدون الذين لديهم مفتاح فك التشفير.

مع وجود العديد من التهديدات عبر الإنترنت التي تعرضنا للخطر، فمن الحكمة استخدام أحد تطبيقات المراسلة الأكثر أمانًا. من المحتمل أن معظم من حولك يستخدم واحدًا، لذلك عليك فقط أن تقرر أي واحد تختاره، بناءً على الأوصاف المذكورة أعلاه.

نصائح حول كيفية تأمين تطبيق المراسلة الخاص بك

تعد الرسائل المشفرة أكثر أمانًا من الرسائل غير المشفرة، ولكن لا يزال يتعين عليك توخي الحذر عند استخدام تطبيقات المراسلة الأكثر أمانًا. اتبع قائمة التحقق هذه للحفاظ على حماية تطبيق المراسلة الخاص بك:

أولاً: كن حذرًا عند استخدام شبكات Wi-Fi العامة. تفتقر هذه الشبكات عادة إلى التدابير الأمنية الأساسية، مما يجعل من السهل على المتسللين التطفل على حركة مرور الويب الخاصة بك.

إذا كنت تستخدم خدمة مراسلة غير مشفرة على شبكة Wi-Fi عامة، فيمكن لمجرمي الإنترنت اعتراض رسائلك وصورك وكلمات مرورك والمعلومات الحساسة الأخرى التي تشاركها. يمكن أن تساعد شبكة VPN الآمنة في حمايتك عن طريق إخفاء حركة المرور الخاصة بك عن المتلصصين ومنع الخروقات الأمنية.

ثانياً: لا تقدم معلومات خاصة من خلال المحادثات. تجنب مشاركة كلمات المرور والمعلومات المصرفية وتسجيلات الدخول وأي معلومات حساسة أخرى من خلال الدردشات. ولا تشارك أبدًا هذا النوع من المعلومات مع الغرباء.

ثالثاً: لا تنقر على الروابط المشبوهة. إذا أرسل إليك شخص لا تعرفه رسالة نصية وأرسل لك رابطًا يبدو بريئًا، فلا تنقر عليه. يُعرف المحتالون عبر الإنترنت بإرسال روابط عشوائية إلى مواقع التصيد الاحتيالي.

رابعاً: استخدم VPN موثوقًا. فهو يقوم بتشفير حركة مرور التطبيق وحركة المرور عبر الإنترنت بشكل فوري وقوي.

يتم تمويل شبكات VPN المدفوعة مثل NordVPN بشكل أفضل للبحث والتطوير في طرق التشفير، لذلك نضمن لك مستوى أعلى من الأمان داخل وخارج التطبيقات التي تستخدمها. تعمل ميزة الحماية من التهديدات الإضافية في NordVPN على الارتقاء بأمانك إلى المستوى التالي من خلال حظر الإعلانات وأجهزة التتبع والبرامج الضارة. كما أنه يقوم بفحص ملفاتك بحثًا عن البرامج الضارة أثناء التنزيل، لذلك يمكنك الاطمئنان إلى أن جهازك لن يصاب بالعدوى حتى إذا قمت بالنقر فوق رابط مشبوه عن طريق الصدفة.

(هنا قامت شركة NordVPN بالتوصية بنفسها في الدراسة كونها من عملت عليها، ولكن هذا لا يعني أنها الأفضل بين تطبيقات VPN، راجع الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنوان – أفضل خدمات VPN 2023 – للمزيد من التفاصيل حول VPN)

لماذا يجب عليك دائمًا استخدام VPN

التشفير التام بين الطرفين ليس مضمونًا. يتم استغلال الأبواب الخلفية داخل التطبيقات المشفرة طوال الوقت. في عام 2020، أعلنت شركة Cellebrite الأمنية (التي يستخدمها مكتب التحقيقات الفيدرالي وشرطة ميانمار والحكومات) أنها تمكنت من التحايل على التشفير الشامل لتطبيق Signal.

تم تحذير WhatsApp بشأن افتقاره إلى النسخ الاحتياطية المشفرة من طرف إلى طرف، وإذا لم تجعل محادثات Telegram الخاصة بك "سرية"، فلن يتم تشفيرها. لذلك، أيًا كان تطبيق المراسلة المشفر الذي تختاره، اجعله أكثر أمانًا عن طريق تشغيل تطبيق NordVPN، الذي يخفي حركة المرور الخاصة بك على الفور عن المتلصصين الذين قد يتربصون في الشبكة.

(هنا قامت شركة NordVPN بالتوصية بنفسها في الدراسة كونها من عملت عليها، ولكن هذا لا يعني أنها الأفضل بين تطبيقات VPN، راجع الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنوان – أفضل خدمات VPN 2023 – للمزيد من التفاصيل حول VPN)

مع تحيات إخواكم في جيش الملاحم الإلكتروني

و

مجلس التعاون الإعلامي الإسلامي

تنصح بمراجعة كتاب الحرب الإلكترونية الجزء الأول – الأمن السيبراني –

من إعداد مجلس التعاون الإعلامي الإسلامي

كما ننصح بمراجعة الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنون

– أفضل خدمات VPN 2023 –